WEST

End of Result Set

Generate Collection Print

L1: Entry 1 of 1 File: DWPI Dec 5, 2001

DERWENT-ACC-NO: 2001-070474
DERWENT-WEEK: 200203

TITLE: Secure handling of information encrypted to a data set for use in computer network, involves granting access to a client to access information if he belongs to one of a groups

INVENTOR: HUGHES, J P

PRIORITY-DATA: 1999US-0260796 (March 1, 1999)

PATENT-FAMILY:

PUB-NO	PUB-DATE	LANGUAGE	PAGES	MAIN-IPC
EP 1159661 A1	December 5, 2001	E	000	G06F001/00
WO 200052558 A1	September 8, 2000	E	037	G06F001/00

INT-CL (IPC): G06 F 1/00; G06 F 12/14

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 :
G06F 1/00, 12/14

A1

(11) International Publication Number: WO 00/52558

(43) International Publication Date: 8 September 2000 (08.09.00)

(21) International Application Number: PCT/US00/05317

(22) International Filing Date: 29 February 2000 (29.02.00)

(30) Priority Data:
09/260,796 1 March 1999 (01.03.99) US

(71) Applicant: STORAGE TECHNOLOGY CORPORATION [US/US]; One StorageTek Drive, MS–4309, Louisville, CO 80028–4309 (US).

(72) Inventor: HUGHES, James P.; 6065 Ware Road, Lino Lakes, MN 55104 (US).

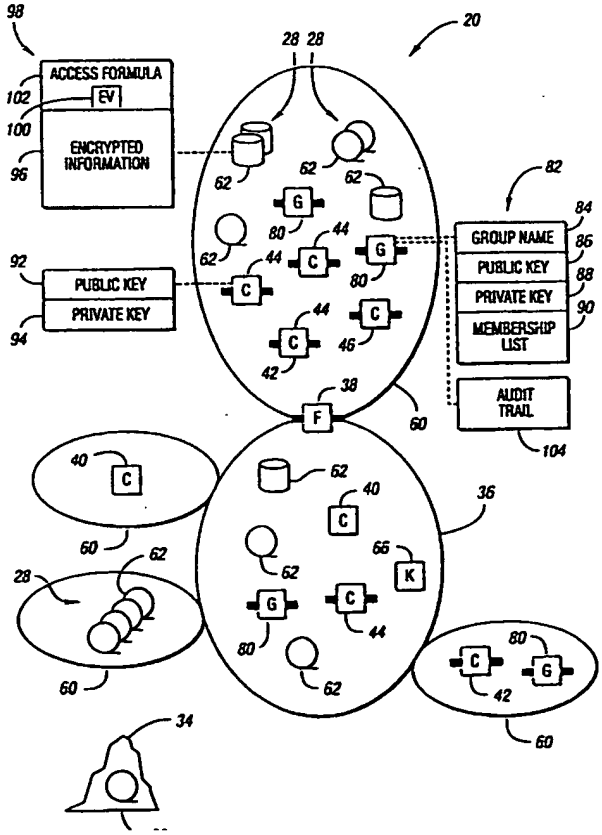
(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: METHOD AND SYSTEM FOR SECURE INFORMATION HANDLING

(57) Abstract

Information that must remain secure is often stored on untrusted storage devices. To increase security, this information is encrypted by an encryption value prior to storing on the untrusted storage device. The encryption value itself is then encrypted. The encryption value is decrypted by correctly solving an access formula describing a function of groups. Each group includes a list of at least one consumer client. A requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula.



WHAT IS CLAIMED IS:

1. A method for the secure handling of information encrypted to a data set, the information requested by a requesting consumer client, the data set stored on at least one storage device, the method comprising decrypting a value required to decrypt the information, the value decrypted by correctly solving an access formula describing a function of groups, each group comprising a list of at least one client, wherein the requesting consumer client is granted access to the information if the requesting consumer client is a member of at least one group which correctly solves the access formula.

2. A method for the secure handling of information as in claim 1 wherein the encrypted value and the access formula are stored as metadata in the data set.

3. A method for the secure handling of information by at least one client using at least one untrusted storage device, each client connected to the at least one untrusted storage device using a network, the network further having a key manager for issuing private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key, the method comprising:

creating at least one group, each group comprising a list of at least one consumer client;

acquiring a public key and a matched private key for each of the at least one group;

encrypting an information set to produce a data set, the encryption based on a randomly generated number;

determining an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a consumer client belonging to the at least one solution group may access the encrypted information set;

asymmetrically encrypting the randomly generated number using the determined access formula and the public key for each of the at least one group granted access to the information set;

adding the encrypted randomly generated number to the data set; and

storing the data set on at least one untrusted storage device.

4. A method for the secure handling of information as in claim 3 wherein a consumer client having a public key and a matched private key requests access to information encrypted in the stored data set, the method further comprising:

receiving a request from the consumer client;

determining if the consumer client belongs to at least one solution group which solves the access formula and, if not, denying access;

otherwise, decrypting the randomly generated number using the private key for the at least one determined solution group; and

encrypting the randomly generated number using the public key for the consumer client thereby permitting access to the encrypted information set by the consumer client.

5. A method for the secure handling of information as in claim 4 further comprising recording all attempts to access the information set in an audit trail, the audit trail including an indication of the consumer client requesting access.

6. A method for the secure handling of information as in claim 3 wherein a plurality of groups form a solution to the access formula, asymmetrically encrypting the randomly generated number creating an encrypted partial key for each group in the plurality of groups, each partial key encrypted using the public key for one group in the plurality of groups, each partial key required to decrypt the encrypted randomly generated number, the method further comprising:

for each group in the plurality of groups, decrypting the encrypted partial key using the private key for the group;

for each group in the plurality of groups, reencrypting the decrypted partial key using the public key for a requesting client;

decrypting each reencrypted partial key using the private key of the requesting client;

determining the randomly generated number based on each partial key; and

decrypting the information set using the determined randomly generated number.

7. A method for the secure handling of information as in claim 3 wherein the access formula is a boolean combination of groups, a group asserting true in the boolean combination when a consumer client member of the group requests access to the information set protected by the access formula, the consumer client group member granted access if the access formula resultant is true.

8. A method for the secure handling of information as in claim 3 further comprising:

determining that an information set destined for storage on at least one untrusted storage device is encrypted; and

prohibiting storage on the at least one untrusted storage device if the information set is determined not to be encrypted.

9. A system for the secure handling of information stored on at least one untrusted storage device connected to a network comprising:

a key manager connected to the network, the key manager operable to generate private key and public key matched pairs for use with an asymmetric encryption and decryption scheme, the scheme allowing a file encrypted with a public key to be decrypted only with a matched private key;

at least one group server connected to the network, each group server operable to

(a) maintain at least one group, each group comprising a list of client members allowed access to information produced by any client member of the group, and

(b) obtain a private key and matched public key for each group; and

at least one producer client connected to the network, the producer client operative to

(a) encrypt an information set to produce a data set, the encryption based on an encryption value,

(b) determine an access formula expressing logical combination of the at least one group for which access to the information set will be granted, solution of the access formula by at least one solution group indicating that a client belonging to the at least one solution group may access the encrypted information set,

(c) asymmetrically encrypt the encryption value using the determined access formula and the public key for each of the at least one group for which access to the information set may be granted,

(d) add the encrypted encryption value and the access formula to the data set, and

(e) store the data set on at least one untrusted storage device.

10. A system for the secure handling of information as in claim 9 wherein the encryption value comprises a randomly generated number.

11. A system for the secure handling of information as in claim 9 wherein the access formula is a boolean combination of groups, a group asserting true in the boolean combination when a client member of the group requests access to the information set protected by the access formula, the client member granted access if the access formula resultant is true.

12. A system for the secure handling of information as in claim 9 wherein the producer client is further operable to

determine that an information set destined for storage on at least one untrusted storage device is encrypted; and

prohibit storage on to the at least one untrusted storage device if the information set is determined not to be encrypted.

13. A system for the secure handling of information as in claim 9 further comprising at least one consumer client connected to the network, each consumer client operative to

obtain a private key and a matched public key;

determine that an accessed data set has encrypted information;

determine at least one group server maintaining at least one group from the access formula logical combination, the at least one group forming a solution to the access formula;

send a request to access the encrypted information set to each of the at least one determined group server;

if access is granted from each of the determined at least one group server, decrypt the encryption value using the obtained private key; and

decrypt the encrypted information set using the decrypted encryption value.

14. A system for the secure handling of information as in claim 13 wherein the at least one group is a plurality of groups and wherein the producer client asymmetrically encrypts the encryption value to produce a partial key for each group in each set of groups forming a solution to the access formula, the consumer client further operative to decrypt the encryption value by decrypting each partial key and to determine the encryption value based on each decrypted partial key.

15. A system for the secure handling of information as in claim 13 wherein each group server is further operable to

receive a request from a requesting consumer client;

determine if the requesting consumer client belongs to at least one solution group which solves the access formula and, if not, deny access;

otherwise, decrypt the encryption value using the private key for the at least one determined solution group; and

encrypt the encryption value using the public key for the requesting consumer client thereby permitting access to the encrypted information set by the consumer client.

16. A system for the secure handling of information as in claim 13 wherein each group server is further operable to record all attempts to access each information set in an audit trail, the audit trail including an indication of the consumer client requesting access.

17. A system for the secure handling of information as in claim 13 wherein each group server is further operable to permit additions, deletions, and changes to each group list of client members.

INTERNATIONAL SEARCH REPORT

Inte. nal Application No
PCT/US 00/05317

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F1/00 G06F12/14

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 787 175 A (CARTER STEPHEN R) 28 July 1998 (1998-07-28) abstract; figures 1-5	1,2
Y		3-5, 9-11,13, 15-17
Y	EP 0 895 149 A (SIEMENS AG) 3 February 1999 (1999-02-03) abstract; figure 3 page 3, column 24, line 35 page 9, column 21, line 34 page 16, column 25, line 30	3-5, 9-11,13, 15-17
A	US 5 696 898 A (GROSSE ERIC ET AL) 9 December 1997 (1997-12-09) column 5, line 6 - line 25	1-17

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 July 2000	02/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Sigolo, A

INTERNATIONAL SEARCH REPORT

Information on patent family members

Int[illegible]ional Application No
PCT/US 00/05317

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5787175 A	28-07-1998	NONE	
EP 0895149 A	03-02-1999	NONE	
US 5696898 A	09-12-1997	CA 2196867 A	07-12-1996
		CN 1159234 A	10-09-1997
		EP 0793826 A	10-09-1997
		WO 9715008 A	24-04-1997